

CLAIMS

What is claimed is:

1. A method comprising:

generating an asymmetric cryptographic key pair comprising first and second keys;

encrypting a boot loader program for a baseband module with said first key;

storing said second key in said baseband module; and

distributing said encrypted boot loader program together with said second key.

2. The method of claim 1, wherein encrypting said boot loader program comprises generating a message digest for said boot loader program and encrypting said message digest with said first key.

3. The method of claim 1, wherein said first key is a private key and said second key is a public key.

4. A method comprising:

receiving a radio protocol at a baseband module;

determining whether said radio protocol has been certified by a certification authority; and

storing said radio protocol in a non-volatile memory device in said baseband module, if said radio protocol has been certified by said certification authority.

5. The method of claim 4, wherein determining whether said radio protocol has been certified comprises authenticating said radio protocol using a first cryptographic key stored in said baseband module.
6. The method of claim 5, wherein said first cryptographic key is a public key.
7. The method of claim 3, wherein said storing said radio protocol comprises using a boot loader program to write said radio protocol to said non-volatile memory device.
8. The method of claim 7, further comprising determining whether said boot loader program has been approved by a manufacturer of said baseband module.
9. The method of claim 8, wherein determining whether said boot loader program has been approved by said manufacturer comprises authenticating said program using a second cryptographic key stored in said baseband module.
10. The method of claim 9, wherein said second cryptographic key is a public key.

11. A method comprising:

generating an asymmetric cryptographic key pair comprising first and second keys;

storing said second key in a non-volatile memory device in a baseband module;

encrypting a radio protocol with said first key, said protocol having been certified by a certification authority; and

distributing said encrypted radio protocol.

12. The method of claim 11, wherein storing said second key comprises authenticating a previously distributed boot loader program which controls access to said non volatile memory device; and using said authenticated boot loader program to write said second key to said non-volatile memory device.

13. The method of claim 12, wherein authenticating said previously distributed boot loader program comprises using a third cryptographic key stored in said baseband module by a manufacturer thereof.

14. The method of claim 12, wherein said first key is a private key and said second key is a public key.

15. The method of claim 11, wherein everything said radio protocol comprises generating a message digest for said radio protocol and encrypting said message digest with said first key.

16. Apparatus comprising:

a receiver to receive a radio protocol;

a mechanism to determine whether said radio protocol has been certified by a certification authority; and

a non-volatile memory device to store said radio protocol if it has been certified by said certification authority.

17. The apparatus of claim 16, wherein said mechanism determines whether said radio protocol has been certified by authenticating said radio protocol using a cryptographic key stored in said baseband module.

18. The apparatus of claim 17, wherein said first cryptographic key is a public key.

19. The apparatus of claim 16, further comprising a boot loader program to write said radio protocol to said non-volatile memory device.

20. The apparatus of claim 19, further comprising a mechanism to determine whether said boot loader program has been approved by a manufacturer of said apparatus.

21. The apparatus of claim 20, wherein said mechanism to determine whether said boot loader program has been approved by a manufacturer of said apparatus authenticates said boot loader program using a second cryptographic key stored in said apparatus.

22. The apparatus of claim 21, wherein said second cryptographic key is a public key.

23. A computer-readable storage medium having stored thereon a sequence of instructions which when executed cause a processor to perform operations comprising:

- receiving a radio protocol at a baseband module;
- determining whether said radio protocol has been certified by a certification authority; and
- storing said radio protocol in a non-volatile memory device in said baseband module, if said radio protocol has been certified by said certification authority.

24. The computer-readable storage medium of claim 23, wherein determining whether said radio protocol has been certified comprises authenticated said radio protocol using a first cryptographic key stored in said baseband module.

25. The computer-readable storage medium of claim 24, wherein said first cryptographic key is a public key.

26. The computer-readable storage medium of claim 23, wherein said storing said radio protocol comprises using a boot loader program to write said radio protocol to said non-volatile memory device.

27. The computer-readable storage medium of claim 26, wherein said operations further comprise determining whether said boot loader program has been approved by a manufacturer of said baseband module.

28. The computer-readable storage medium of claim 27, wherein determining whether said boot loader program has been approved by said manufacturer comprises authenticating said program using a second cryptographic key stored in said baseband module.

29. The computer-readable storage medium of claim 27, wherein said second cryptographic key is a public key.

30. Apparatus comprising:
means for receiving a radio protocol;
means for determining whether said radio protocol has been certified by
certification authority; and
means for storing said radio protocol if it has been certified by said
certification authority in non-volatile memory.

31. The apparatus of claim 9, wherein said means for determining whether
said radio protocol has been certified authenticate said radio protocol using a
cryptographic key stored in said baseband module.

32. The apparatus of claim 30, wherein said first cryptographic key is a public
key.

33. The apparatus of claim 29, further comprising a boot loader means for
writing said radio protocol to said memory device.

34. The apparatus of claim 32, further comprising a means for determining
whether said boot loader means has been approved by a manufacturer of said
apparatus.

